CHICAGO TITLE™

INFORMATION SECURITY OFFICE

October
is National Cybersecurity Awareness Month

Chicago Title Company wishes to remind all our employees, contractors, affiliates and customers that this October is National Cybersecurity Awareness Month. It is the 15th year as an annual initiative to raise awareness about the importance of cybersecurity and is a collaborative effort between government and industry to ensure every American has the resources they need to stay safer and more secure online, while increasing the resiliency of the Nation during cyber-threats. As part of our ongoing mission to promote cybersecurity, we will be presenting important information regarding cybersecurity at home, cybersecurity in the workplace and careers in cybersecurity in the coming weeks.

Cybersecurity at Home

Internet Crime has no boundaries as all Americans from every age-group seem to be equally affected - Even Bubba could be a victim of cyber-crime

Home computer users have been victims of unprecedented cyber-crime over the past decade. Recent exploits of home computer users include Ransomware, Identity Theft, Harassment and Extortion. The primary means of delivering cyber attacks against home users is the Internet and statistically, no age group is immune either. For more information, go to the FBI 2017 Internet Crime Report at https://pdf.ic3.gov/2017_IC3Report.pdf.

There are many things you can do to prevent cyber-crime. Check out these useful links for making your computer and Online data more secure:

10 Ways to Secure a New Computer
https://www.us-cert.gov/ncas/tips/ST15-003

Virus Basics
https://www.us-cert.gov/publications/virus-basics

Choosing and Protecting Passwords
https://www.us-cert.gov/ncas/tips/ST04-002

Home Network Security
https://www.us-cert.gov/ncas/tips/ST15-002

Mobile Device Security

Mobile Devices such as smart phones and tablets have become the new computers-of-choice for millions of Americans and introduce entirely new threats to one's identity and information. As a rule of thumb in the cybersecurity community, all mobile devices are considered "untrusted devices" by their very nature. The number of apps available for Android and iOS operating systems, which constitute the largest share of mobile devices, have exploded offering users everything from real-time traffic information to Online banking. However, cybersecurity professionals have struggled to keep up with the ability to secure these devices and the apps that use them. The primary threats to mobile users are:

Malicious Apps (Mobile Malware): there are a significant number of apps that are specifically designed to infect the user's mobile device such as Trojan software (a type of computer worm). These malicious apps intentionally steal data from other apps on the phone (such as contacts), steal data form files on the device such as photo's and videos, allow cyber-criminals to intercept calls and text messages and allow malicious actors to turn on cameras and record sounds.

Insecure Apps: It is estimated that over 80% of all mobile apps have significant vulnerabilities that could lead to exploitation by cyber-criminals leading to data loss and device compromise.

Insecure WiFi Exploitation: There are many applications designed to trick users to log into them posing as WiFi hot-spots. Once connected, these applications, called Remote Access Tools (RATs), can hijack the entire mobile device and compromise all of its data.

Protecting Your Mobile Device - Helpful Links

Check out the following links for information that can help you protect your mobile devices and information:

Best Practices: Securing Your Mobile Device

https://www.trendmicro.com/vinfo/us/security/news/mobile-safety/best-practices-securing-your-mobile-device

10 Best Ways to Secure Your Android Phone

https://www.zdnet.com/article/the-ten-best-ways-to-secure-your-android-phone/

 iPhone Security Tips

https://www.macworld.co.uk/how-to/iphone/iphone-security-tips-3638233/

Social Media Security Concerns

Social Media sites have grown in popularity over the past decade and have offered an avenue for people to connect in ways that were unimaginable in previous generations. The ability to allow users to share photo's, videos and intimate personal information does not come without risk. Modern Social Media sites have introduced new considerations for cybersecurity from cyber-bullying to privacy concerns where anyone from cyber-criminals to large corporations can have access to your personal information.

For information on how to stay safe on social media visit: https://www.us-cert.gov/ncas/tips/ST06-003

Online Shopping Security

Online Commerce has exploded in growth over the past 15 years providing more choices and convenience for customers than ever before. From monolithic Online retail sites such as Amazon to small businesses providing niche products and services there is no doubt that Online shopping is here to stay. As such, cyber-criminals have concentrated significant efforts in compromising Online shopping sites and your shopping data through various means. StaySafeOnline (powered by the National Cybersecurity Alliance) has published valuable information for consumers to stay safe when shopping Online. For more information go to:

https://staysafeonline.org/stay-safe-online/online-safety-basics/online-shopping/

Banking and Finance Online

It is almost impossible to find any bank or major financial institution that does not offer Online portals for customers to do just about everything from checking their balance, paying bills and investing in the stock market. As with Online shopping, or any type of action that could compromise financial data for that matter, cyber-criminals have historically targeted banks and Online financial applications.

Although consumers cannot control how financial institutions secure their data, there are steps you can do to help protect your financial information when banking Online:

13 Essential Online Banking Tips

https://www.tomsguide.com/us/pictures-story/1148-online-banking-security-tips.html